WHAT IS CLAIMED IS:

1. An encryption apparatus for a common-key cipher, comprising:

a unit for generating a plurality of plaintext blocks P_i ($1 \leq i \leq N$) resulting from separating a plaintext on a specific-length basis, the plaintext including redundant data and a message;

an encryption operation unit for generating a random-number string R from a secret key,

generating random-number blocks R_i ($1 \leq i \leq N+1$) from the random-number string R, and

performing an encryption operation for ciphertext blocks C_i ($1 \leq i \leq N+2$) by using the plaintext blocks P_i ($1 \leq i \leq N$) and the random-number blocks R_i ($1 \leq i \leq N+1$), the random-number string R being longer than the plaintext, the random-number blocks R_i ($1 \leq i \leq N+1$) being used for the encryption corresponding to the plaintext blocks P_i ($1 \leq i \leq N$); and

an authentication operation unit for

generating random-number blocks R_i ($2 \leq i \leq N+1$) from the random-number string R, and

performing an authentication operation for message-authentication-code blocks by using the ciphertext blocks C_i ($1 \leq i \leq N+2$) and the random-number blocks R_i ($2 \leq i \leq N+1$), the random-number blocks R_i ($2 \leq i \leq N+1$) being used for the authentication corresponding to the ciphertext blocks C_i ($1 \leq i \leq N+2$).

2. The encryption apparatus for a common-key

cipher according to Claim 1, wherein

the encryption operation unit and the authentication operation unit use the one or more random-number blocks R_i ($1 \leq i \leq N+1$),

the total-sum length of the one or more random-number blocks R_i ($1 \leq i \leq N+1$) being longer than the total-sum length of the plaintext blocks P_i ($1 \leq i \leq N$), and being shorter than two times the total-sum length of the plaintext blocks P_i ($1 \leq i \leq N$).

3. The encryption apparatus for a common-key cipher according to Claim 2, wherein

the encryption operation unit performs a binomial operation or a monomial operation one or more times in accordance with predetermined processing steps, the binomial operation or the monomial operation using the plaintext blocks P_i ($1 \leq i \leq N$),

the authentication operation unit performing a binomial operation or a monomial operation one or more times in accordance with predetermined processing steps, the binomial operation or the monomial operation using the ciphertext blocks C_i ($1 \leq i \leq N+2$),

the encryption apparatus for a common-key cipher further comprising a unit for combining the plurality of acquired ciphertext blocks C_i ($1 \leq i \leq N+2$) with the message-authentication-code blocks, and outputting the combined result as a ciphertext.

4. The encryption apparatus for a common-key cipher according to Claim 2, wherein

the encryption operation unit performs the encryption operation by an exclusive-OR logical sum,

the authentication operation unit performing the authentication operation by an arithmetic multiplication and an arithmetic addition.

5. The encryption apparatus for a common-key cipher according to Claim 2, wherein

the encryption operation unit performs the encryption operation by an exclusive-OR logical sum,

the authentication operation unit performing the authentication operation by a multiplication on a finite field and an arithmetic addition.

6. The encryption apparatus for a common-key cipher according to Claim 2, wherein

the encryption operation unit and the authentication operation unit share the random-number blocks R_i ($1 \leq i \leq N+1$) used by the encryption operation unit and the authentication operation unit.

7. The encryption apparatus for a common-key cipher according to Claim 2, wherein

the encryption operation unit and the authentication operation unit use the random-number blocks R_i ($1 \leq i \leq N+1$) which differ from each other.

8. The encryption apparatus for a common-key cipher according to Claim 2, further comprising a pseudo random-number generation unit for generating the random-number string R from said secret key.

9. The encryption apparatus for a common-key

cipher according to Claim 8, further comprising:

a unit for dividing the message into a plurality of messages, the psuedo random-number generation unit generating the random-number string R whose random numbers are equivalent to the divided messages in number; and

a unit for allocating either of the divided messages and the random-number string R to different operation units each, and thereby causing a parallel processing to be performed.

10. A decryption apparatus for a common-key cipher, comprising:

a unit for generating a plurality of ciphertext blocks C'_i ($1 \leq i \leq N+2$) resulting from separating a ciphertext on a specific-length basis;

an authentication operation unit for

generating a random-number string R from a secret key,

generating random-number blocks R_i ($1 \leq i \leq N+1$) from the random-number string R, and

performing an authentication operation for message-authentication-code blocks by using the ciphertext blocks C'_i ($1 \leq i \leq N+2$) and the random-number blocks R_i ($1 \leq i \leq N+1$), the random-number string R being longer than the ciphertext, the random-number blocks R_i ($1 \leq i \leq N+1$) being used for the authentication corresponding to the ciphertext blocks C'_i ($1 \leq i \leq N+2$); and

a decryption operation unit for

generating random-number blocks R_i ($1 \leq i \leq N$) from the random-number string R, and

performing a decryption operation for plaintext blocks P'_i ($1 \leq i \leq N$) by using the ciphertext blocks C'_i ($1 \leq i \leq N+2$) and the random-number blocks R_i ($1 \leq i \leq N$), the random-number blocks R_i ($1 \leq i \leq N$) being used for the decryption corresponding to the ciphertext blocks C'_i ($1 \leq i \leq N+2$).

11. The decryption apparatus for a common-key cipher according to Claim 10, wherein

the authentication operation unit and the decryption operation unit use the one or more random-number blocks R_i ($1 \leq i \leq N+1$),

the total-sum length of the one or more random-number blocks R_i ($1 \leq i \leq N+1$) being longer than the total-sum length of the plaintext blocks P'_i ($1 \leq i \leq N$), and being shorter than two times the total-sum length of the plaintext blocks P'_i ($1 \leq i \leq N$).

12. The decryption apparatus for a common-key cipher according to Claim 11, further comprising:

a unit for connecting the plurality of plaintext blocks P'_i ($1 \leq i \leq N$) thereby to generate a plaintext;

a unit for extracting redundant data included in the plaintext; and

a unit for checking the redundant data thereby to detect the presence or absence of a forgery

that may have been performed to the ciphertext.

13. A program-storing medium which stores a program for allowing a computer to execute an encryption processing for a common-key cipher, wherein

the program allows the computer

to generate a plurality of plaintext blocks P_i ($1 \leq i \leq N$) resulting from separating a plaintext on a specific-length basis, the plaintext including redundant data and a message;

to generate a random-number string R from a secret key,

to generate random-number blocks R_i ($1 \leq i \leq N+1$) from the random-number string R, and

to perform an encryption operation for ciphertext blocks C_i ($1 \leq i \leq N+2$) by using the plaintext blocks P_i ($1 \leq i \leq N$) and the random-number blocks R_i ($1 \leq i \leq N+1$), the random-number string R being longer than the plaintext, the random-number blocks R_i ($1 \leq i \leq N+1$) being used for the encryption corresponding to the plaintext blocks P_i ($1 \leq i \leq N$); and

to generate random-number blocks R_i ($2 \leq i \leq N+1$) from the random-number string R, and

to perform an authentication operation for message-authentication-code blocks by using the ciphertext blocks C_i ($1 \leq i \leq N+2$) and the random-number blocks R_i ($2 \leq i \leq N+1$), the random-number blocks R_i ($2 \leq i \leq N+1$) being used for the authentication corresponding to the ciphertext blocks C_i ($1 \leq i \leq N+2$).

14. The program-storing medium according to Claim 13, wherein

the encryption operation and the authentication operation use the one or more random-number blocks R_i ($1 \leq i \leq N+1$),

the total-sum length of the one or more random-number blocks R_i ($1 \leq i \leq N+1$) being longer than the total-sum length of the plaintext blocks P_i ($1 \leq i \leq N$), and being shorter than two times the total-sum length of the plaintext blocks P_i ($1 \leq i \leq N$).

15. The program-storing medium according to Claim 14, wherein

the program allows the computer

to perform, as the encryption operation, a binomial operation or a monomial operation one or more times in accordance with predetermined processing steps, the binomial operation or the monomial operation using the plaintext blocks P_i ($1 \leq i \leq N$);

to perform, as the authentication operation, a binomial operation or a monomial operation one or more times in accordance with predetermined processing steps, the binomial operation or the monomial operation using the ciphertext blocks C_i ($1 \leq i \leq N+2$); and

to combine the plurality of acquired ciphertext blocks C_i ($1 \leq i \leq N+2$) with the message-authentication-code blocks, and to output the combined result as a ciphertext.

16. The program-storing medium according to Claim

14, wherein

the program allows the computer

to perform the encryption operation by an exclusive-OR logical sum, and

to perform the authentication operation by an arithmetic multiplication and an arithmetic addition.

17. The program-storing medium according to Claim 14, wherein

the program allows the computer

to perform the encryption operation by an exclusive-OR logical sum, and

to perform the authentication operation by a multiplication on a finite field and an arithmetic addition.

18. The program-storing medium according to Claim 14, wherein

the program allows the encryption operation and the authentication operation to share the random-number blocks R_i ($1 \leq i \leq N+1$) used by the encryption operation and the authentication operation.

19. The program-storing medium according to Claim 14, wherein

the program allows the computer to perform a pseudo random-number generation processing for generating the random-number string R from said secret key.

20. The program-storing medium according to Claim 19, wherein

the program allows the computer

to divide the message into a plurality of messages;

to generate, by the psuedo random-number generation processing, the random-number string R whose random numbers are equivalent to the divided messages in number; and

to allocate either of the divided messages and the random-number string R to different operation units each, and thereby to perform a parallel processing.

21. A program-storing medium which stores programs for allowing a computer to execute a decryption processing for a common-key cipher, wherein

the program allows the computer

to generate a plurality of ciphertext blocks C'_i ($1 \leq i \leq N+2$) resulting from separating a ciphertext on a specific-length basis;

to generate a random-number string R from a secret key,

to generate random-number blocks R_i ($1 \leq i \leq N+1$) from the random-number string R, and

to perform an authentication operation for message-authentication-code blocks by using the ciphertext blocks C'_i ($1 \leq i \leq N+2$) and the random-number blocks R_i ($1 \leq i \leq N+1$), the random-number string R being longer than the ciphertext, the random-number blocks R_i ($1 \leq i \leq N+1$) being used for the authentication

corresponding to the ciphertext blocks C'_i ($1 \leq i \leq N+2$); and

to generate random-number blocks R_i ($1 \leq i \leq N$) from the random-number string R, and

to perform a decryption operation for plaintext blocks P'_i ($1 \leq i \leq N$) by using the ciphertext blocks C'_i ($1 \leq i \leq N+2$) and the random-number blocks R_i ($1 \leq i \leq N$), the random-number blocks R_i ($1 \leq i \leq N$) being used for the decryption corresponding to the ciphertext blocks C'_i ($1 \leq i \leq N+2$).

22. The program-storing medium according to Claim 21, wherein

the program allows the decryption operation and the authentication operation to use the one or more random-number blocks R_i ($1 \leq i \leq N+1$),

the total-sum length of the one or more random-number blocks R_i ($1 \leq i \leq N+1$) being longer than the total-sum length of the plaintext blocks P'_i ($1 \leq i \leq N$), and being shorter than two times the total-sum length of the plaintext blocks P'_i ($1 \leq i \leq N$).

23. The program-storing medium according to Claim 22, wherein

the program allows the computer

to connect the plurality of plaintext blocks P'_i ($1 \leq i \leq N$) thereby to generate a plaintext;

to extract redundant data included in the plaintext; and

to check the redundant data thereby to detect

the presence or absence of a forgery that may have been performed to the ciphertext.